UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,167	12/05/2003	Thomas A. Crispin	CNTR.2224-C1	2865

23669 7590 11/03/2009

HUFFMAN LAW GROUP, P.C.
1900 MESA AVE.
COLORADO SPRINGS, CO 80906

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
11/03/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO@HUFFMANLAW.NET

Office Action Summary	Application No.	Applicant(s)	
	10/730,167	CRISPIN ET AL.	
	Examiner	Art Unit	
	Thomas Gyorfi	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 August 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22,24,25,27,56-64,66-76 and 79-83* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22,24,25,27,56-64,66-76 and 79-83* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22, 24, 25, 27, 56-64, 66-76, and 79-83 remain for examination. The correspondence filed 8/23/09 amended claims 1, 6, 11-13, 56, 60, 66, & 67.

Response to Arguments

2. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection. However, for the record Examiner wishes to remind Applicant that patent references are not limited to their description of their own inventions but are relevant for all they contain (*In re Heck*, 699 F.2d 1331-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) quoting *In re Lemelson*, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968))). A reference may be relied upon for all that it would have reasonably suggested to one of ordinary skill in the art, including non-preferred embodiments (*Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ 1843 (Fed. Cir.) *cert. denied*, 493 U.S. 975 (1989)). See also MPEP 2123. In this case, the particulars of Best's cryptographic coprocessor and how they may or may not differ from the cryptographic coprocessor of Kessler's disclosure is not at issue. Rather, Examiner has been consistent in taking the position that, in previous iterations of the claims, the Kessler coprocessor process cryptographic instructions in accordance with each and every pertinent limitation of at least the independent claims; if not for the fact that the claims specifically recite a microprocessor having said features rather than a coprocessor, Kessler would have anticipated the claims. However, Best suggests that a coprocessor may be joined with a conventional microprocessor to create a hybrid

microprocessor capable of both conventional microprocessor functionality and dedicated cryptographic functionality. Even if the details of Best's coprocessor differ from Kessler's, this teaching is enough to reasonably suggest to one of ordinary skill in the art might have been able to combine other types of cryptographic coprocessors with conventional microprocessors in much the same way that Best did. One of ordinary skill in the art would be further buoyed by the mutually-agreed upon fact that this type of combination has occurred previously in the history of the x86 architecture (amendment of 8/23/09, page 23, third paragraph), illustrating that the technique was within the capability of one of ordinary skill in the art. Finally, in response to Applicant's argument that because there is no prior art teaching currently on the record explicitly disclosing an x86-compatible processor with a dedicated cryptographic functional unit in the thirty years since the Best reference was filed (amendment, pages 23-24), courts have held that the age of a reference does not preclude a finding of obviousness, absent a showing that the prior art tried and failed to solve the same problem notwithstanding its presumed knowledge of the references (In re Wright, 569 F.2d 1124, 193 USPQ 332 (CCPA 1977)). Applicant has shown no evidence that anyone tried and failed to make an x86-compatible CPU with a dedicated cryptographic functional unit prior to the instant invention, thus Applicant's allegation is insufficient to overcome the rejection.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1-6, 11, 12, 24, 25, 27, 56-60, 66, and 79-83 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler et al. (U.S. Patent 6,789,147) in view of Bakhle et al. (U.S. Patent 6,021,201) in view of Best (U.S. Patent 4,278,837).

Regarding claim 1:

Kessler discloses a processor apparatus for performing a cryptographic operation, the apparatus comprising: fetch logic, configured to fetch an instruction flow from memory for execution by a processor (col. 4, line 59 – col. 5, line 36), said instruction flow comprising an instruction, configured to direct said processor to perform the cryptographic operation (col. 4, lines 10-16; col. 5, lines 29-36; Figure 7), wherein said cryptographic instruction prescribes one of the cryptographic operations (Figure 3); said cryptographic operation comprising: an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory (element 302 of Fig. 3; col. 5, lines 37-50); and a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data (element 310 of Fig.3; col. 5, line 50 – col. 6, line 10); and a cryptography unit, disposed within execution logic in said processor, configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word (col. 9, lines 7-55); and an integer unit, disposed within execution logic in said processor and coupled in parallel

with said cryptography unit, configured to execute a plurality of integer operations that are required to accomplish the cryptographic operation (col. 9, lines 15-20).

Kessler does not explicitly disclose wherein the cryptographic instructions to be executed are atomic in nature. However, Bahkle discloses a related cryptographic coprocessor that implemented this limitation (col. 5, lines 15-25). It would have been obvious to one of ordinary skill in the art to ensure the atomic operation of the cryptographic instructions executed by the Kesller processor; one would have been motivated to do so because it prevents the various functional units within said processor from overwriting shared memory buffers and thus corrupting the results produced by other operations being performed within said processor (col. 12, lines 15-30).

The processor disclosed by Kessler is a coprocessor, which by itself does not conform to Applicant's preferred definition of "microprocessor" established in the specification. However, Best discloses wherein microprocessors with dedicated cryptographic functionality could be employed in an apparatus, wherein said microprocessor is a hybrid consisting of a conventional microprocessor and a cryptographic coprocessor combined into one single, indivisible microprocessor that behaves in exactly the manner as the "microprocessor" of the instant application (col. 19, lines 20-60; Figures 17 & 18). Additionally, Best clearly discloses wherein the microprocessor has a fetch unit disposed within itself configured to fetch an application program from memory by said microprocessor (e.g. col. 6, lines 15-20). The claims are thus obvious because the substitution of Kessler's cryptographic coprocessor in lieu of the default cryptographic coprocessor already disclosed by Best for use as the

cryptographic unit of Best's hybrid microprocessor would have yielded predictable results to one of ordinary skill in the art by the time of the instant invention.

Best places no limitations as to the specific architecture employed by the prior art microprocessor functional unit of the hybrid microprocessor; nevertheless, Examiner takes Official Notice that, given the ubiquity of the x86 architecture as well as past instances where the general technique of integrating a coprocessor into an x86-based microprocessor had previously been practiced in the art, that it would have been immediately obvious to use an x86-compatible microprocessor as the prior art microprocessor unit of the Best invention [in view of Kessler]. Pursuant to MPEP 2144.03, see the Wikipedia reference entered into the record on 6/4/08: page 2, "History" and "Design"; as well as page 4, 3rd paragraph.

Regarding claim 56:

Kessler discloses an apparatus for performing cryptographic operations, comprising: fetch logic, disposed within a processor, configured to fetch an instruction flow from memory for execution by a processor by said processor (col. 4, line 59 – col. 5, line 36), said instruction flow comprising an instruction, configured to direct said processor to perform the cryptographic operation (col. 4, lines 10-16; col. 5, lines 29-36; Figure 7), wherein said cryptographic instruction prescribes one of the cryptographic operations (Figure 3); said cryptographic operation comprising: an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory (element 302 of Fig. 3; col. 5, lines

37-50); and a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data (element 310 of Fig.3; col. 5, line 50 – col. 6, line 10); translation logic, disposed within said processor, configured to translate said cryptographic instructions into associated micro instructions that specify sub operations required to accomplish said one of the cryptographic operation (e.g. col. 8, lines 11-16); and a cryptography unit, disposed within execution logic in said processor, configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word (col. 9, lines 7-55).

Kessler does not explicitly disclose wherein the cryptographic instructions to be executed are atomic in nature. However, Bahkle discloses a related cryptographic coprocessor that implemented this limitation (col. 5, lines 15-25). It would have been obvious to one of ordinary skill in the art to ensure the atomic operation of the cryptographic instructions executed by the Kesller processor; one would have been motivated to do so because it prevents the various functional units within said processor from overwriting shared memory buffers and thus corrupting the results produced by other operations being performed within said processor (col. 12, lines 15-30).

The processor disclosed by Kessler is a coprocessor, which by itself does not conform to Applicant's preferred definition of "microprocessor" established in the specification. However, Best discloses wherein microprocessors with dedicated

cryptographic functionality could be employed in an apparatus, wherein said microprocessor is a hybrid consisting of a conventional microprocessor and a cryptographic coprocessor combined into one single, indivisible microprocessor that behaves in exactly the manner as the "microprocessor" of the instant application (col. 19, lines 20-60; Figures 17 & 18). Additionally, Best clearly discloses wherein the microprocessor has a fetch unit disposed within itself configured to fetch an application program from memory by said microprocessor (e.g. col. 6, lines 15-20). The claims are thus obvious because the substitution of Kessler's cryptographic coprocessor in lieu of the default cryptographic coprocessor already disclosed by Best for use as the cryptographic unit of Best's hybrid microprocessor would have yielded predictable results to one of ordinary skill in the art by the time of the instant invention.

Best places no limitations as to the specific architecture employed by the prior art microprocessor functional unit of the hybrid microprocessor; nevertheless, Examiner takes Official Notice that, given the ubiquity of the x86 architecture as well as past instances where the general technique of integrating a coprocessor into an x86-based microprocessor had previously been practiced in the art, that it would have been immediately obvious to use an x86-compatible microprocessor as the prior art microprocessor unit of the Best invention [in view of Kessler]. Pursuant to MPEP 2144.03, see the Wikipedia reference entered into the record on 6/4/08: page 2, "History" and "Design"; as well as page 4, 3rd paragraph.

Regarding claims 2 and 83:

Kessler further discloses wherein the cryptographic operations are accomplished at the level of system privileges afforded to application programs (SSL being a component of web browser applications: col. 4, lines 5-10).

Regarding claims 3 and 57:

Kessler further discloses an encryption operation encrypting a plurality of blocks of input data to generate a plurality of ciphertext blocks (e.g. col. 2, lines 13-14 etc.)

Regarding claims 4 and 58:

Kessler further discloses an decryption operation decrypting a plurality of blocks of input data to generate a plurality of plaintext blocks (Ibid).

Regarding claims 5 and 59:

Kessler further discloses using AES (col. 9, lines 13-15; Figure 8, element 807).

Regarding claims 6 and 60:

Kessler further discloses a block cipher mode to be employed in accomplishing the cryptographic operations (inherent to the block ciphers taught in col. 9, lines 10-20).

Regarding claim 11:

Kessler further discloses wherein the atomic instruction proscribes that the cryptographic operations be accomplished on a plurality of text blocks (Figure 7)

Regarding claims 12 and 66:

It is now taken as an admission of prior art that the "prior art microprocessor" component of the hybrid microprocessor disclosed by Best would be an x86 processor, with instructions prescribed in the x86 instruction format; even were that not so, it should be logically self-evident that an x86 compatible processor employed as the prior art microprocessor of Best could inherently process x86 instructions.

Regarding claims 24 and 79:

Kessler further discloses block cipher logic, configured to perform a plurality of cryptographic rounds on each of said plurality of blocks of input data according to said one of the block cryptographic operations to produce said corresponding plurality of output text blocks (col. 9, lines 7-44); and key RAM, operatively coupled to said block cipher logic, configured to store a key schedule, said key schedule comprising a plurality of round keys, each corresponding to a plurality of cryptographic rounds, and configured to provide each of said plurality of round keys to said block cipher logic for performance of said each of said plurality of cryptographic rounds (col. 9, lines 23-55).

Regarding claims 25 and 80:

Kessler further discloses wherein said block cipher logic id divided into two or more stages, whereby said plurality of cryptographic rounds are simultaneously performed on two or more of said plurality of blocks of data (inherent to at least the AES and 3DES algorithms disclosed on col. 9, lines 10-20).

Regarding claims 27 and 82:

Kessler further discloses wherein said opcode field directs said cryptography unit to load one of said each of said plurality of input text blocks and to perform said plurality of cryptographic rounds (col. 5, lines 40-50).

Regarding claim 81:

Kessler further discloses an integer unit, coupled in parallel with said cryptography unit, configured to execute a plurality of integer operations that are required to accomplish the cryptographic operations (arithmetic unit: col. 9, lines 15-20).

5. Claims 7-10 and 61-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler in view of Bakhle in view of Best as applied to claims 6 and 60 above, and further in view of the "Applied Cryptography, 2nd Edition" (hereinafter, "Schneier").

Regarding claims 7-10 and 61-64:

Although Kessler and Best both disclose using block cipher modes for at least some of the supported encryption algorithms, they do not explicitly mention any of the modes listed in these claims. However, Schneier teaches that each mode (ECB, CBC, CFB, and OFB) were well known in the art (pages 193-206); accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use any of these modes in the cryptographic processor disclosed by Kessler, let alone the

hybrid of Best modified by Kessler; each mode has its own particular advantages as disclosed by Schneier (page 209, as appropriate).

6. Claims 13-22 and 67-76 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler in view of Bakhle in view of Best as applied to claims 1 and 56 above, and further in view of Johns-Vano et al. (U.S. Patent 6,026,490).

Regarding claims 13 and 67:

Although Kessler and Best both disclose at least one register (Kessler: element 220 of Figure 2; Best: col. 5, lines 35-50 and Figures 8 & 9), it is unclear as to whether the instruction implicitly references a plurality of registers in the device. However, Johns-Vano discloses that the instruction set of a cryptographic processor implicitly references a plurality of internal registers (elements 558, 560, 564, 552, 566, and 556 of Figure 1). It would have been obvious to one of ordinary skill in the art at the time the invention was made for a cryptographic processor to employ a plurality of registers. One would do so because using hardware registers would be conducive to making a cryptographic processing engine suitable for manufacture in semiconductor foundries thereby reducing manufacturing costs (col. 2, lines 28-33). It is also noted that x86 processors were already known to have registers (e.g. Wikipedia, pages 2-3).

Regarding claims 14 and 68:

Johns-Vano further discloses a first register, wherein contents of said first register comprise a pointer to a first memory address, said first memory address specifying a first location in said memory for access of a plurality of input text blocks upon which the cryptographic operations is to be accomplished (col. 5, lines 1-55).

Regarding claims 15 and 69:

Johns-Vano further discloses a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing the cryptographic operations upon a plurality of input text blocks (col. 5, lines 1-55).

Regarding claims 16 and 70:

Johns-Vano further discloses a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks (col. 5, lines 1-55).

Regarding claims 17 and 71:

Johns-Vano further discloses a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address

specifying a third location in said memory for access to cryptographic key data for use in accomplishing the cryptographic operations (col. 5, lines 1-55).

Regarding claims 18 and 72:

Kessler and Johns-Vano further disclose wherein said cryptographic key data comprises a cryptographic key (Kessler: col. 6, lines 40-50; Johns-Vano: col. 7: 1-5).

Regarding claims 19 and 73:

Kessler further discloses wherein said cryptographic key data comprises a cryptographic key schedule (inherent to the algorithms used in col. 9, lines 10-20).

Regarding claims 20 and 74:

Johns-Vano further discloses a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in said memory for access of an initialization vector for use in accomplishing the cryptographic operations (col. 5, lines 1-55).

Regarding claims 21 and 75:

Johns-Vano further discloses a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in said memory for access of said control word for use in

accomplishing the cryptographic operations, wherein said control word prescribes cryptographic parameters for cryptographic operations (col. 5, lines 1-55).

Regarding claims 22 and 76:

Kessler further discloses an encryption/decryption field, configured to prescribe whether the cryptographic operation is an encryption operation or a decryption operation (col. 5, lines 50-60).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: "WPI Cryptography and Information Security reference" establishes that enabling a conventional microprocessor with an extended cryptographic instruction set was an alternative to employing a dedicated cryptographic coprocessor (see page 1, Abstract, 1st paragraph).

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
10/26/09
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435